

FTC in Three

Facial Recognition Technology October 26, 2012

Cheryl Hackley (Off Camera): Welcome to this week's edition of FTC in Three. Our topic today is facial recognition technology. Recently, the FTC released a staff report on best practices for businesses using this technology. Today we have Amanda Koulousias with us to take questions. Amanda is a staff attorney in the FTC's Division of Privacy and Identity Protection. Welcome Amanda.

Amanda Koulousias (On Camera): Thanks! Happy to be here.

Cheryl: Our first question comes from Twitter. @RandyPicker asks: Are we allowed to try to recognize the people who are broadcast on camera?

Amanda: Thank you for your question. First, I would like to just give a reminder that the FTC report is not an interpretation of laws that the FTC enforces, but rather examples of best practices. The report does not allow or prohibit particular actions, but simply contains recommendations for companies that want to use facial recognition in a privacy-sensitive manner.

In the commercial context, FTC staff recommends that as a best practice companies should not use facial recognition to identify an individual to someone who couldn't otherwise identify them, unless they have obtained that individual's consent. Therefore, in the scenario you describe, the best practice would be for the company to use facial recognition to identify only those individuals who have given their consent to being identified.

Cheryl: Great! Thanks, Amanda. Securix recently posted a review of the report's recommendations and asked the following questions: What makes biometric data so special? Should the same standards apply to all personal data or just pictures of faces?

Amanda: That's a good question. The recommendations for best practices that in the facial recognition report are based on the three core principles in the FTC's March 2012 Privacy Report which are: privacy by design, simplified consumer choice, and transparency. The Privacy Report also addressed the issue of what types of data should be covered by those principles. In that report, the FTC stated that commercial entities should implement privacy protections for any data that can be reasonably linked to a specific consumer, computer or device. Biometric data and pictures of consumers faces fall within that scope because they can reasonably be linked to a specific consumer.

In terms of whether biometric data is special or whether the same standards should apply to all personal data, it depends upon the recommendation. For example, while companies should have reasonable data security protections for all data – what is reasonable may be different for depending upon the type of data. For instance, biometric data, such as a "faceprint" extracted from a photo, may call for stronger data security protections than other types of information because biometric data is typically a persistent identifier that cannot be changed or replaced if it

is compromised. Other recommendations, such as that companies get a consumer's affirmative express consent before using data in a different manner than they represented when they collected the data, apply no matter what type of personal data is at issue.

Cheryl: Here's a general question several people have posed online: Why are you recommending best practices now if companies aren't currently misusing facial recognition technologies?

Amanda: Recommending best practices at this point provides benefits to both companies and consumers that want to use facial recognition technologies. The fact that the commercial use of facial recognition technologies is still developing in certain contexts presents a unique opportunity to give guidance to companies that want to develop their products and services with privacy in mind, allowing companies to build privacy protections into their products and services at the outset as opposed to after the fact. Facial recognition products and services can also provide many benefits to consumers, such as the ability to organize photos or to virtually try on different products online – and some consumers may be more likely to take advantage of those benefits if the products were designed in a privacy-sensitive manner.

Cheryl: Great, thanks for joining us this week, Amanda!

Amanda: Closing remark

Cheryl: Next week our guest is David Vladeck, Director of the FTC's Bureau of Consumer Protection. Check out [FTC.gov/ftcinthree](https://www.ftc.gov/ftcinthree) for information on how to submit your questions to David.